

## ⑫ 公開特許公報(A)

昭64-73449

⑬ Int.Cl.<sup>4</sup>G 06 F 15/00  
9/06

識別記号

3 3 0

庁内整理番号

7361-5B  
B-7361-5B

⑭ 公開 昭和64年(1989)3月17日

審査請求 未請求 発明の数 1 (全5頁)

⑮ 発明の名称 暗証番号入力方式

⑯ 特 願 昭62-230851

⑰ 出 願 昭62(1987)9月14日

⑱ 発 明 者 宍 道 徹 夫 茨城県日立市大みか町5丁目2番1号 株式会社日立コー  
トロールシステムズ内

⑲ 出 願 人 株式会社日立製作所 東京都千代田区神田駿河台4丁目6番地

⑳ 出 願 人 株式会社日立コントロ 茨城県日立市大みか町5丁目2番1号  
ールシステムズ

㉑ 代 理 人 弁理士 鶴沼 辰之 外1名

## 明 細 書

## 1. 発明の名称

暗証番号入力方式

## 2. 特許請求の範囲

1. データを入力し、該データに基づく出力を表示する端末と、該端末よりの前記データにより、所定の判断、所定の出力を行う演算手段と、乱数を生じ該演算手段に出力する乱数発生手段と、データ加工ルールを格納し該演算手段に出力するルール格納手段と、前記データを記憶し該演算手段に出力する記憶手段とからなり、前記端末への特定操作により、前記演算手段は、該特定操作に基づく情報を前記記憶手段に記憶させると共に前記乱数発生手段に乱数を生じさせ、該乱数を前記端末に表示して前記情報に対応した前記データ加工ルールにより前記乱数の加工を要求し、この要求により前記端末に入力された第1加工データと、前記記憶手段に記憶された前記情報により前記ルール格納手段から該情報に対応したデータ加工ルールを入力して

前記乱数を加工して第2加工データを作成し、前記第1加工データと該第2加工データとを比較して一致した場合前記第1データを正しい暗証番号と判断することを特徴とする暗証番号入力方式。

2. 前記特定操作に基づく情報が、業務の識別記号であることを特徴とする特許請求の範囲第1項記載の方式。

3. 前記特定操作に基づく情報が、所定の前記端末に対する起動操作であることを特徴とする特許請求の範囲第1項記載の方式。

## 3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は、暗証番号入力方式に係り、特に端末を使用する際、特定の許可された人物であることを確認するための暗証番号入力方式に関する。

〔従来の技術〕

従来例の1つは、特開昭61-128368号に記載のように、端末から入力するときのキーの配列を暗証番号を入力するたびに变化させることにより、

他人から操作しているキーの位置を見られても、暗証番号そのものは覚えられないようにしていた。

しかし、キーの配置は変化するが、キーそのものは一定であり、入力しているキー（すなわち、3とか5の数字）を他人に見られると、その時点で暗証番号を盗まれることになるという欠点があった。

従来例の他の1つは、特開昭61-157975号に開示されており、予め登録されている暗証番号に1桁ないしはそれ以上の桁数の暗証番号を追加する方式であるが、この追加された暗証番号は、入力する日付のデータの一部（例えば、日にちの1桁目）を使用することにより、もし入力している暗証番号を他人に見られても、この暗証番号は別の日には無効になるというものである。しかし、日付データから追加の暗証番号を決めているために、同一の日にはこの暗証番号が悪用できるという欠点をもつ。

〔発明が解決しようとする問題点〕

上記のように、従来技術は、他人に端末入力操

作を見られたときはも、完全に暗証番号の機密性を保持することができなかった。

本発明は、入力している暗証番号そのものを見られても、他人に悪用されることを防ぐ暗証番号入力システムを提供することにある。

〔問題点を解決するための手段〕

上記問題点は、データを入力し、該データに基づく出力を表示する端末と、該端末よりの前記データにより、所定の判断、所定の出力を行う演算手段と、乱数を発生し該演算手段に出力する乱数発生手段と、データ格納ルールを格納し該演算手段に出力するルール格納手段と、前記データを記憶し該演算手段に出力する記憶手段とからなり、前記端末への特定操作により、前記演算手段は、該特定操作に基づく情報を前記記憶手段に記憶させるとともに、前記乱数発生手段に乱数を発生させ、該乱数を前記端末に表示して前記情報に対応した前記データ加工ルールにより前記乱数の加工を要求し、この要求により前記端末に入力された第1加工データと、前記記憶手段に記憶された前

記情報により前記ルール格納手段から該情報に対応したデータ加工ルールを入力して前記乱数を加工して第2加工データを作成し、前記第1加工データと該第2加工データとを比較して一致した場合、前記第1加工データを正しい暗証番号と判断する暗証番号入力方式により解決される。

〔作用〕

予め、データ加工ルールを知っている操作者が端末に特定操作を行うと、演算手段は、該特定操作に基づく情報を記憶手段に記憶させるとともに、乱数発生手段に対して乱数を発生させ、この乱数を前記端末に表示して、操作者に対し前記情報と対応した予め知っているデータ加工ルールと前記乱数とから第1加工データを作成して端末に入力することを要求し、前記記憶手段に記憶された前記情報に対応したデータ加工ルールを、ルール格納手段から入力して前記第2加工データを作成し、該第2加工データを前記第1加工データとを比較して一致した場合、前記第1加工データを正しい暗証番号と判断する。

〔実施例〕

以下、本発明の第1実施例を、第1図～第3図により説明する。

第1図は第1実施例の暗証番号入力システムのブロック図を示す。

計算機1の端末2よりデータ入力あるいは問合わせ等を行う際、オペレータが端末操作、すなわちこれから行おうとする業務の認識記号（以下、業務IDと称す）を入力する。計算機1の中の演算処理装置3は、端末入出力装置4を経由して、この業務IDを取り込み記憶装置7に格納し、端末2に「暗証番号を入力して下さい」のメッセージを出力する。この際、乱数発生ルーチン6により無作為の英数字列を作成して端末2に表示すると同時に、記憶装置7に格納する。オペレータは、予め知らされている加工ルールにより表示された英数字列を加工し、その結果を暗証番号として端末2から入力する。演算処理装置3は、この暗証番号を端末入出力装置4経由で取り込む。すでに入力されている業務IDを記憶装置7から取り出し、

これに対応する加工ルールを、ルール格納ファイル5から選び出す。また、記憶装置7からすでに端末に表示されている英数字列を取り出し、業務IDに対応する加工ルールにより加工する。加工の具体例としては、加工ルールごとのサブルーチンを準備し、業務IDとそれに対応する加工サブルーチン群を、ルール格納ファイル5に収納しておく。

演算処理装置3は、取り出した英数字列を業務IDに対応する加工サブルーチンに渡し、このサブルーチンにて所定のルールにより英数字列を加工する。この結果と、入力された暗証番号を演算処理装置3にて照合し、一致すれば以降の処理に入り、一致しなければ暗証番号不適切ということで、処理を打ち切る。以上の処理を、第2図の流れ図に示す。第3図を用いて、乱数発生ルーチンにて作成された英数字列と、加工ルールの例を説明する。

業務ID8である20を入力した例を示す。計算機より毎回変わる数字列9（この例の場合、

5931）が表示される。オペレータは、予め加工ルール「1000の位と1の位の差の絶対値を数字列の各桁の数字にそれぞれ加える。加えた結果が10を越えたときには、その1桁目の数字を使う」を知っており、この例の場合9375を入力する。もし、この入力した数字を第三者に見られても、その人間が同じ業務IDで端末操作したときには、今度は5931とは異なる値、例えば、0742が表示されるため、正しい暗証番号は2964となり、9375ではエラーとなる。

次に、第2実施例を第4図、第5図により説明する。第1実施例では、初めに業務IDを端末2から入力し、この業務IDに対応する加工ルールにより暗証番号を決定しているが、入力する端末2により加工ルールを定めることも可能である。すなわち、オペレータが端末2に向って所定のシステム起動操作、例えばLOGINを行つたところで英数字列を表示して、暗証番号入力をうながす。オペレータは、端末2に対応した加工ルールにより暗証番号を決定し、これを入力する。計算

機は、入力された端末番号から加工ルールを選び出し、暗証番号が正しいかどうか確認する。

また、銀行の現金引き出し装置のように使用される業務がすべて同じであり、また位置の端末からの入力を許すような場合は、暗証番号に固定部と可変部を設けることにより、本発明が実施できる。

第4図は、暗証番号に固定部と可変部を設けた第3実施例を示す図である。

利用者が端末2の操作を始めると、まず、「暗証番号を入力して下さい」というメッセージが端末に表示される。このメッセージに引き続いて、乱数発生ルーチンにより作られた無作為の英数字列が表示される。

ここで、利用者は端末から暗証番号を入力することになるが、暗証番号は第4図の例に示すごとく、固定部13と可変部14とからなる。第4図の例では、5H3、079がそれぞれ固定部13である。固定部13の暗証番号と可変部14を作り出すための加工ルールは一義的に対応しており、

これは予め利用者だけに知らされている。

利用者は、暗証番号の固定部13をまず入力し、その後引き続いて可変部14を、表示された英数字列11と加工ルールから決定し入力する。加工ルールは、例えば、第4図の暗証番号例2の場合固定部13が5H3のときには、「表示された数字列の最上位の値を、下位4桁の数字にそれぞれ加えた4桁の数字列」となつていとする。表示された数字列11の最上位の値は1であり、下位4桁の数字は4462であることから、4462の各桁の数字に1を加えた5573がこの場合の正しい数字列となる。

利用者が固定部5H3に続いて可変部5573を入力すると、コンピュータはすでに表示した英数字列と、入力された暗証番号の固定部13から加工ルールを選び出し、加工ルールにより可変部14の値を算出、この値と入力された可変部14の暗証番号を照合することにより、正しい利用者であるかどうか判断する。

第5図に、この一連の流れを示す。第4図の時

証番号の例2では、固定部13の値が0、79であり、これに対応する加工ルールは、「表示された数字列の最下位から2番目の値を上位4桁の数字からそれぞれ減算した4桁の数字列、ただし減算するとマイナスの値となる場合には、10をたす」とする。第4図にて表示される数字列11は、1384462であるため、最下位から2番目の値は6となり、上位4桁の数字は1384となる。各桁より6を減算し、マイナスになったときには10を加えると、得られる数字は5728となる。

万一、5H35573あるいは0795728の暗証番号を入力しているところを他人に見られても、この暗証番号はコンピュータから表示された英数字列1384462に対応しているものであり、この英数字列は暗証番号を入力するたびに無作為されるため、同じ英数字列が表示される確率は極めて低く、一度見られた暗証番号を悪用されることを防止できる。

#### 〔発明の効果〕

本発明によれば、データ加工ルールを予め操作

者と記憶装置に記憶しておき、操作者が端末に特定操作を行うと、その特定操作に基づく情報により、演算手段は乱数を発生し表示して、操作者によりその乱数と予め知っているデータ加工ルールから第1加工データを作成させて入力させ、一方、前記情報に対応したデータ加工ルールと前記乱数とにより第2加工データを作成し、この第2加工データと第1加工データとを比較して一致した場合、第1加工データを正しい暗証番号と判断するので、入力している暗証番号そのものを他人に見られても、データ加工ルールを知らないこの他人は、この番号を暗証番号として使用することができないという優れた効果がある。

#### 4. 図面の簡単な説明

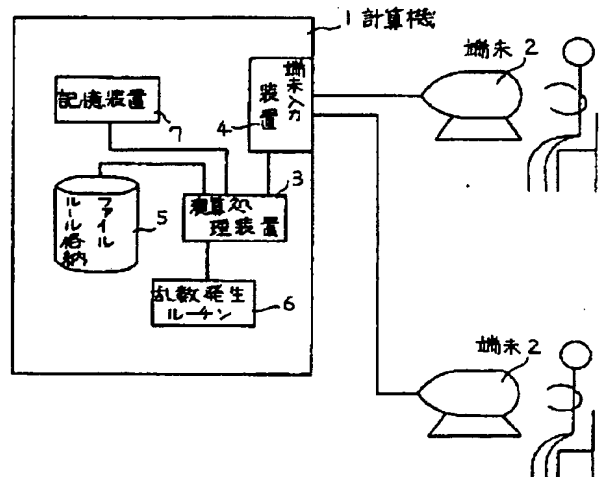
第1図は本発明のシステムブロック図、第2図は暗証番号を処理する流れを示す図、第3図は暗証番号加工ルールの例を示す図、第4図は暗証番号に固定部と可変部とを設けた実施例を示す図、第5図は第4図の処理の流れを示す図である。

1…計算機、2…端末、3…演算処理装置、4…

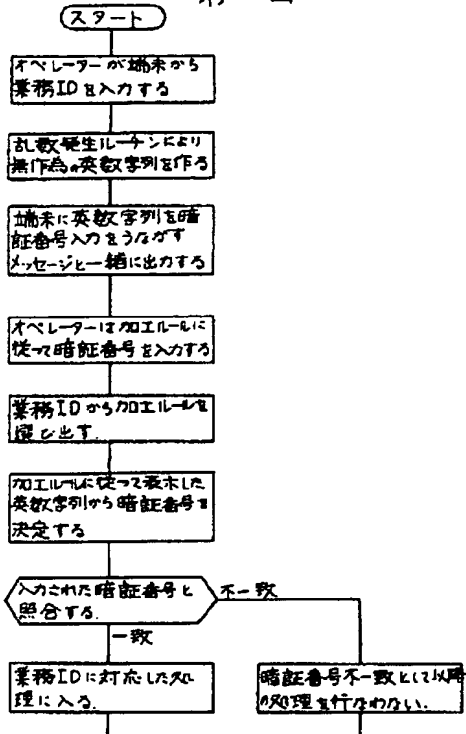
端末入出力装置、5…ルール格納ファイル、6…乱数発生ルーチン、7…記憶装置。

代理人 弁理士 鶴沼辰之

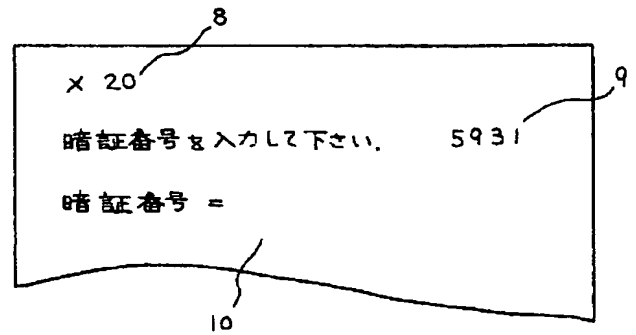
第1図



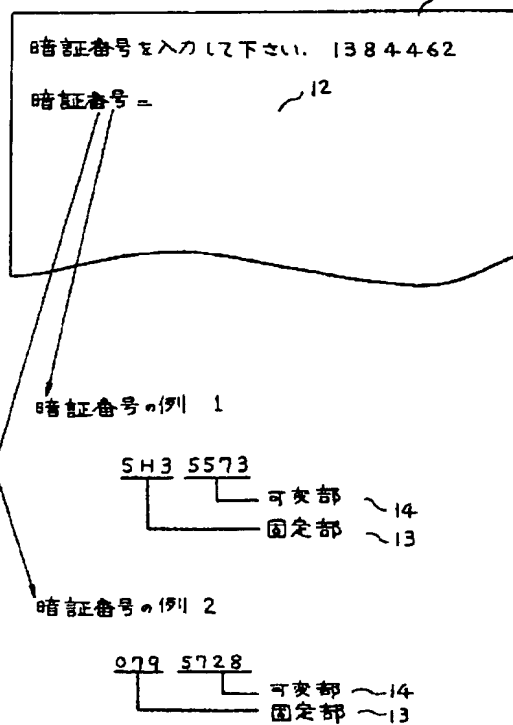
第2図



第3図



第4図



第5図

